BY ORDER OF THE COMMANDER
AIR FORCE SPECIAL OPERATIONS COMMAND

AFSOC INSTRUCTION 33-303
1 JANUARY 2000

Communications and Information

AFSOC WEB PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFSOC WWW site at: www.afsoc.af.mil/library. If you lack access, contact the OPR to obtain a copy.

OPR: HQ AFSOC/SCMN (GS-11 Brenda Bowman)
Certified by: HQ AFSOC/SCMN (GS-12 Mary Waxler)
Pages: 13
Distribution: F

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 37-1, *Air Force Information Management* (will convert to AFPD 33-3); AFPD 35-2, *Public Communications Programs*; AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*; and AFPD 33-2, *Information Protection*. It establishes Air Force Special Operations Command (AFSOC) procedures for requesting and posting information to the SIPRNet and NIPRNet. It does not apply to the Air Force Reserve (AFRC) and to the Air National Guard (ANG) units.

1. Purpose. Use of the Internet has dramatically increased in popularity as a means of obtaining and disseminating information worldwide. This document addresses those unique characteristics of web use and technology pertinent to AFSOC as a command and its individual units for both the classified and unclassified networks (SIPRNet and NIPRNet). Failure to observe the prohibitions and mandatory provisions of this instruction by military personnel is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal sanctions for violations of related laws.

2. Discussion. Web technology at AFSOC is used to propagate information to remote units, local personnel, and the general public. Because so many people in different places can access the information, our goal as information providers is to maximize the availability of timely and accurate information, as well as to maintain a secure framework for our use of Internet-based technologies.

3. Web Responsibilities. Several entities within the AFSOC command have responsibilities regarding administration of the AFSOC Web. The list below names the usual entities responsible for web oversight and administration; however, depending on the situation other individuals might be called upon to assist. Delegation letters for each of the appointed Web Oversight Group (WOG) positions should be forwarded to the WOG chairman.

3.1. Web Oversight Group (WOG) Composition**.** The WOG has the final approval authority on the publishing of AFSOC Web pages for the SIPRNet and NIPRNet. The Web Oversight Group

convenes as necessary (at least quarterly) to review active web pages. The WOG also approves (usually by E-mail) new and major updates to pages prior to being posted on the AFSOC Website. When major revisions (major/minor revisions are defined in paragraph 3.3.5.1. and 3.3.5.2.) or additions to a web page are required, the unit webmaster will simultaneously forward the revisions to all personnel comprising the WOG for review. When the review is complete, the webmaster will notify the page maintainer. Minor revisions can be incorporated by the webmaster; however, major revisions will be accomplished by the page maintainer. The WOG composition is normally those officers listed below at MAJCOM, Wing, or Group level as appropriate. However, during quarterly web page reviews or if deemed necessary, unit page maintainers or unit subject matter experts (SME) will augment the WOG.

3.1.1. Senior Systems Manager. The communications unit network flight (or equivalent) shall provide a representative for the WOG. This representative serves as the chairman of the WOG and will be responsible for compiling requirements, promulgating agendas, minutes, and action items as required for the WOG.

3.1.2. OPSEC (Operational Security). The MAJCOM/Wing/Group OPSEC representative will be part of the Web Oversight Group. This representative must be well-versed on current OPSEC procedures and considerations.

3.1.3. INFOSEC (Information Security). The MAJCOM/Wing/Group INFOSEC representative should be familiar with all aspects of Information Security as it relates to the Special Operations Command and current operational trends and considerations.

3.1.4. STINFO (Scientific and Technical Information). A formally trained STINFO representative should be part of the WOG. In the absence of a trained representative, a person knowledgeable in Export Arms regulations will be part of all WOG activities.

3.1.5. Privacy Act/ Freedom of Information Act (FOIA). The MAJCOM, Wing, or Group FOIA Officer (as appropriate) will be part of the WOG and will be the point of contact for Privacy Act or FOIA matters. Should a conflict or question arise, the MAJCOM FOIA Officer should be the deciding authority.

3.1.6. Intelligence. Intelligence functions from the corresponding MAJCOM, Wing or Organization will provide a representative to review web content for Essential Elements of Friendly Information (EEFI). EEFIs are key questions likely to be asked by adversary officials and intelligence systems about friendly intentions, capabilities, and activities, in order to obtain answers critical to their operational effectiveness.

3.1.7. Public Affairs Officer (PAO). Normally the final approval authority for NIPRNet web pages, the PAO will be represented at all levels in the WOG. PA personnel at their corresponding units will review materials to be posted to the NIPRNet or SIPRNet following the criteria outlined in this instruction.

3.1.8. Webmaster. As the person who actually posts most web pages, the AFSOC Webmaster will be part of all WOG activities. Duties and responsibilities for the webmaster are further discussed in paragraph 3.3. below.

3.2. As the individual body within each AFSOC unit that ultimately has the responsibility to review and approve pages for that entity, the HQ/Wing/Unit WOG duties are as follows:

3.2.1. Formally review all web pages for content, sensitivity, and distribution/release controls, including sensitivity of information in the aggregate, prior to placement on the web.

3.2.2. Conduct a review of all of the organization's posted web pages (SPIRNet and NIPRNet) quarterly. This review should be scheduled for 25% of the pages at any one time, four times annually.

3.2.3. Seek guidance from the Legal Office in matters concerning copyright violations, etc.

3.2.4. Ensure all WOG members are trained in OPSEC and INFOSEC procedures.

3.2.5. Ensure information is safeguarded at the appropriate level.

3.2.6. Ensure the Internet is used for legal and ethical purposes in the best interest of the DoD.

3.3. Webmaster. The webmaster will:

3.3.1. Maintain the site's top-level home pages, ensuring internal navigation links and links to the outside are operational and comply with appropriate instructions.

3.3.2. Post pages to the server after they have been reviewed and approved by the WOG.

3.3.3. Maintain a copy of the accountability package for each group of web pages in accordance with AFMAN 37-139. This package will be unclassified and will include the AF Form 3215 (Attachment 2) and the checklist for approving information on AFSOC Web pages (Attachment 3).

3.3.4. Design and develop web pages for those units within their wing or group without resources to develop their own.

3.3.5. Determine whether changes to existing pages constitute a major or minor revision.

3.3.5.1 Minor Revisions. Unit web pages, which require small changes or additions, are considered minor revisions. These changes include updating information or making small additions to clarify existing information and will be evaluated on a case-by-case basis.

3.3.5.2. Major Revisions. Unit web pages, which require extensive changes or significant additions, are considered major revisions. This includes adding new web page groups (i.e. an LGM division to the LG web page) and new unit web pages. Major revisions will be approved by the WOG, who will review them as a convening group or via E-mail coordinated by the Webmaster. Once all WOG members have approved all changes, the webmaster will file a copy of the accountability package and the pages will be posted.

3.3.6. Maintain a record of which pages have been reviewed. This record will be provided as necessary to ensure all pages are reviewed at least once per year.

3.4. Page Maintainers. A representative from each unit will be designated to supplement the WOG. This representative will serve as point of contact for the webmaster, for making changes or additions to the unit's web pages and for technical information regarding the unit's web pages. Each page maintainer is responsible for maintaining the original accountability package of their web pages in accordance with AFMAN 37-139.

3.5. Web Server Administration. AFSOC has the unique circumstance where, at many sites, the server administration is not done by the AFSOC unit webmaster. In these instances, it is up to the host web administration personnel to ensure the site is managed in accordance with AFI 33-129. However, if the AFSOC pages reside on that server, the webmaster/page maintainer for the AFSOC unit will:

3.5.1. Ensure the security, access, and operation of the server are in accordance with appropriate instructions.

3.5.2. Ensure all links from pages under their control are appropriate and valid.

3.5.3. Establish procedures for page maintainers to place information on the web server.

3.5.4. Maintain a copy of the accountability packages for the all pages posted.

3.5.5. Ensure security and access controls requested by page maintainers are implemented.

3.6. Web Users. All AFSOC personnel should remain aware of the information accessed via the internet. They should question anything that seems out of the ordinary. Should a question arise as to appropriateness of any posted materials, they should contact the unit webmaster or the PAO regarding the releasability or suitability of information posted.

4. Requirements Processing. Follow AFI 33-103, *Requirements Development and Processing*, when there is a need to place information on a web server, or develop information to be placed on a web page. Attachment 2 summarizes the requirements and provides an example of a C4 Systems Requirements Document (AF Form 3215) filled out as a request for web pages. If the directorate wishes to design their own web page, this can also be done. Guidelines can be obtained from the AFSOC Webmaster regarding design and content. Attachment 3 provides a

checklist to be followed when designing a web page for publication on the AFSOC Website. When completed, the package will be submitted to the WOG who will review the page for content and design. Once approved, the webmaster will post the page on the appropriate webserver.

5. System Security. There are several ways of restricting information from the general public. Among them are domain restriction, password protection, and encryption. It should be understood that there is no restriction considered 100% secure on the Internet. Therefore, classified information and FOR OFFICIAL USE ONLY (FOUO) will **NOT** be put on the AFSOC NIPRNet site. Currently, two methods of safeguarding information from unauthorized disclosure are used in the NIPRNet AFSOC Website: Domain restriction and Password protection.

5.1. Domain Restriction (.mil Only Access). Domain restriction is one way of ensuring information is not available to the general public. Pages that require restriction will be put in a specified directory or partition where only URLs originating at bases with URL's ending in .mil (i.e., www.afsoc.af.mil) will be allowed access. However, there are several ways to spoof .mil only protection. Also, certain universities have access to .mil only domains, or the page could be accessed from libraries or other buildings within military installations that are accessible to the public. But overall, the information is protected from the general public.

5.2. Password Protection. Password protection is available to protect information that is required by a small number of people. It should be pointed out that passwords transferred via unencrypted telephone lines are subject to monitoring and the use of "sniffers" (software that looks for specific patterns or words with a transmission such as "password"). The server administrator should be contacted to set up a password protected site.

JOHN W. MALUDA, Colonel, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS AND TERMS

Section A--References.

AFI 33-129, Transmission of Information via the Internet

Directive Number 25-71, USSOCOM Guidance for the Implementation, Maintenance and Security of World Wide Web (WWW) Sites

DEPSECDEF Memorandum: Web Site Administration Policies & Procedures, dated November 25, 1998

Section B--Acronyms and Abbreviations

AFI	Air Force Instruction
AFSOC	Air Force Special Operations Command
FOIA	Freedom of Information Act
INFOSEC	Information Security
NIPRNet	UNclassified Internet Protocol Router Network
OPSEC	Operational Security
PAO	Public Affairs Officer
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SOCOM	Special Operations Command
STINFO	Scientific and Technical Information
WOG	Web Oversight Group

Section C--Terms.

Group Web Pages	Pages belonging to one directorate or group (i.e. LGS pages)
Major Revision	A revision that affects over 10% of the particular web page or one that implements a new policy or directive, or provides significant new information.
Minor Revision	A revision that affects less than 10% of the particular web page, one that is a “pen and ink” change, or one that will not have a significant impact on the information contained on the web site.
Major Command (MAJCOM)	A major subdivision of the Air Force that is assigned a major part of the Air Force mission. MAJCOMs report directly to

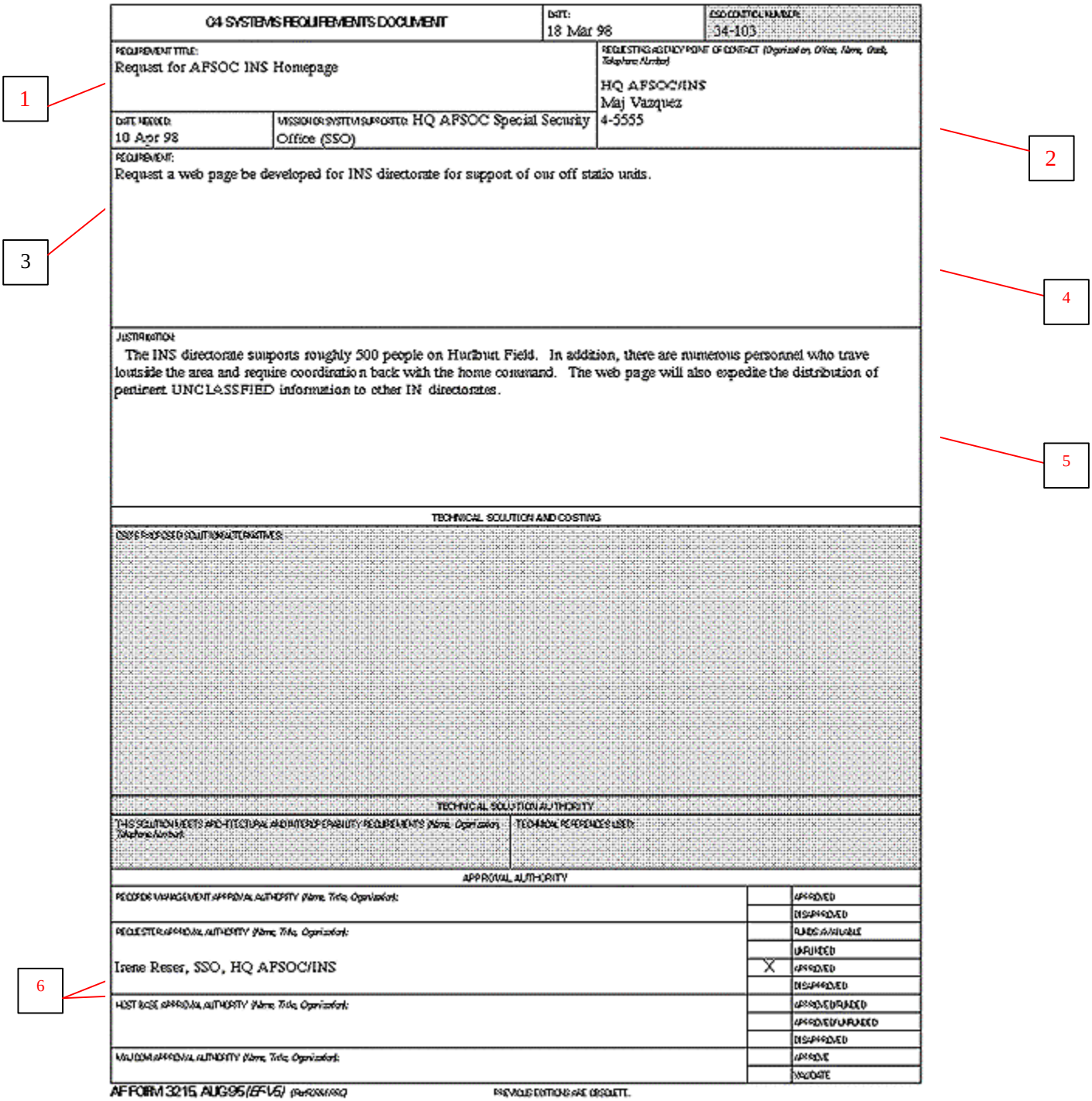
HQ USAF.

C4 System — An integrated combination of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all operational phases. It includes base visual information support systems.

Attachment 2

INSTRUCTIONS FOR FILLING OUT A REQUEST FOR WEB PAGE / WEB SPACE

Figure 1 is a sample C4 SYSTEMS REQUIREMENTS DOCUMENT that should be filled out whenever there is a requirement for space on the web server to post a web page. The following are required fields:



C4 SYSTEMS REQUIREMENTS DOCUMENT

DATE: 18 Mar 98

ESD CONTROL NUMBER: 34-103

REQUIREMENT TITLE: Request for AFSOC INS Homepage

REQUESTING AGENCY POINT OF CONTACT (Organization, Office, Name, Grade, Telephone Number): HQ AFSOC/INS, Maj Vazquez, 4-5555

DATE NEEDED: 10 Apr 98

MISSION OR SYSTEM SUPPORTED: HQ AFSOC Special Security Office (SSO)

REQUIREMENT: Request a web page be developed for INS directorate for support of our off static units.

JUSTIFICATION: The INS directorate supports roughly 500 people on Hurlburt Field. In addition, there are numerous personnel who trave loutside the area and require coordinatio n back with the home command. The web page will also expedite the distribution of pertinent UNCLASSFIED information to other IN directorates.

TECHNICAL SOLUTION AND COSTING

COST & PROPOSED SOLUTION/ALTERNATIVES:

TECHNICAL SOLUTION AUTHORITY

THIS SOLUTION MEETS ARCHITECTURAL AND INTEROPERABILITY REQUIREMENTS (Name, Organization, Telephone Number):

TECHNICAL REFERENCES USED:

APPROVAL AUTHORITY

RECORDS MANAGEMENT APPROVAL AUTHORITY (Name, Title, Organization):		APPROVED
		DISAPPROVED
REQUESTER APPROVAL AUTHORITY (Name, Title, Organization):		FUNDS AVAILABLE
		UNFUNDED
Irene Reser, SSO, HQ AFSOC/INS	X	APPROVED
		DISAPPROVED
HOST BASE APPROVAL AUTHORITY (Name, Title, Organization):		APPROVED/FUNDED
		APPROVED/UNFUNDED
		DISAPPROVED
MAJCOM APPROVAL AUTHORITY (Name, Title, Organization):		APPROVE
		VALIDATE

AF FORM 3215, AUG 95 (EF-V5) (PerFORMPRO) PREVIOUS EDITIONS ARE OBSOLETE.

BLOCKS:

1. Requirement Type - Just indicate whether the requirement is for a unit (i.e 720th) or specific function or organization (i.e. FOIA, Y2K) or division (i.e. SCMN).

2. Requesting Agency POC – Should include a name and point of contact for the request. Be aware that each directorate has a Web Affairs point of contact that should be consulted before submitting this request.

3. Date Needed – The latest date that this request can be filled.

4. Requirement – This block should indicate whether the request is for the design of a web page or whether the directorate will design the web page and it will be submitted to the unit/wing/group webmaster for posting. If design is required, include information here that will assist in the design. The webmaster will contact you to get details, but a short description of what will be required should be included here.

5. Justification – Self-explanatory.

6. Requester Approval Authority – The unit cc/director's signature should appear here.

Attachment 3

CHECKLIST FOR APPROVING INFORMATION ON AFSOC WEB PAGES

SECTION I:

Web page title: _____

Web Uniform Resource Locator (URL) address: _____

Classification:
- ☐ UNCLASSIFIED
- ☐ INTRANET
- ☐ CLASSIFIED

Level _____

Access Requested:
- ☐ Limited .mil access
- ☐ Public

Coordination (name, office symbol, date):

Unit/Directorate OPSEC _____
Unit Commander/Director _____
HQ SC / Unit Webmaster _____
Wing/Group Public Affairs _____
(UNCLASS Only)

Page POC:

Name, rank, title _____
Duty Phone _____
Email address _____
Office symbol _____

SECTION II. INFORMATION REVIEW CHECKLIST: Please complete and provide with required documents (i.e. developed pages, information for page development, etc.)

#	ITEM	Yes	No
1.	Does this material contain:		
	a. Any classified information?		
	b. Any lessons plans ?		
	c. Any contract proposals, bids, and/or proprietary information that would prohibit release?		
	d. Any studies or after action reports containing advice and recommendations?		
	e. STINFO information, state-of-the-art or breakthrough technology not public releasable?		
	f. Reference to any information that would reveal sensitive movements of		

	military assets or the location of units, installations, or personnel where uncertainty of location is an element of security of a military plan or program?		
	g. Links to areas that are outside the mission or functional area of the OPR, including commercial organizations		
	h. Copyrighted material, including graphics and artwork?		
	i. "Under Construction" displays or references?		
	k. Commercial logos or trademarks, or distributes commercial software (is it a violation of copyright or licenses), or shareware without formal approval?		
2.	Does the main page contain OPR name, organization, office symbol, commercial phone number, DSN number, email address, public warning banners and applicable disclaimers or restrictions?		
3.	Does this material reveal any security practices or procedures?		
4.	Would release of this information allow development of countermeasures to the applicable system/technology?		
5.	Does the release of this information conflict in any way from AFSOC OPSEC goals?		
6.	Is there any Privacy Act information (SSN's, Personal phone numbers, any dependent information, dates or places of birth, etc.) included in this material for release? (If yes, indicate if material is to be under .mil protection, password protection, or why not.)		
7.	Is this information AFSOC owned information? (If no, owner permission is required.)		
	Is coordination with another military activity required? (If yes, include their concurrence.)		
8.	Does this material contain sensitive information concerning an overall communications-electronics architecture of a tactical, strategic, or sustaining base application?		
9.	Is the webmaster designing this page(s)? (If no, coordination with the webmaster is required for style/background information)		
10.	Have all links been validated, including those within pages and to other sites?		
11.	Commander/Director has approved information.		
12.	Are page maintainers filing a copy of the accountability package for each page(s)?		
13.	(CLASSIFIED ONLY) Are all materials appropriately marked IAW classification Directives?		

SECTION III. REVIEW CERTIFICATION:

As the originating activity, we have reviewed this information to ensure it may be presented, released, and/or published as requested on this form and in accordance with OPSEC, INFOSEC, STINFO, Privacy Act and Freedom of Information Act directives.

- Checklist must be re-certified as accurate and current at least yearly. Web pages should be reviewed at least yearly to ensure compliance with appropriate directives, policy letters and guidance. (USSOCOM Directive 25-71, USSOCOM Guidance for the Implementation, Maintenance and Security of World Wide Web [www] Sites; AFI 33-129, Transmission of Information via the Internet; current DOD policy.)
- Any updates, amendments or changes to page information must be coordinated before adding to web sites.
- Public affairs only approves information being placed on unclassified public web sites. Information coordination applies to content of text, appropriateness of graphics and photos. Public affairs provides security and policy review to determine the degree of releasability only; actual release of material is the decision of the release authority (normally the senior organization or installation commander, or their designee).

_____

REVIEWER

SECTION IV. PUBLIC AFFAIRS/POSTING OFFICER APPROVAL/ DISAPPROVAL:

_____	_____	_____
APPROVED/ DISAPPROVED	SIGNATURE	DATE

Public Affairs

As the person posting this form on the AFSOC web, I have reviewed this form and all accompanying information and certify that it complies with existing AFSOC regulatory requirements for OPSEC, INFOSEC, STINFO, and Public Affairs/FOIA.

_____	_____
WEBMASTER/POSTING OFFICIAL	DATE

Attachment 3